Available online at www.sciencedirect.com
SciVerse ScienceDirect
Procedia Computer Science 16 (2013) 844 – 852
Procedia
Computer Science

Conference on Systems Engineering Research (CSER'13)
Eds.: C.J.J. Paredis, C. Bishop, D. Bodner, Georgia Institute of Technology, Atlanta, GA, March 19-22, 2013.

Empirical Findings about Risk and Risk Mitigating Actions from a Legacy Archive of a Large Design Organization

Chuck Hsiao[a], Richard Malak[a,*], Irem Y. Tumer[b], Toni Doolen[b]

[a]*Texas A&M University, College Station, TX 77843, USA*
[b]*Oregon State University, Corvallis, OR 97331, USA*

Abstract

Understanding how to mitigate project risk is an important aspect of project management. Risks that are not properly managed can lead to cost overruns, schedule delays, wasted manpower and effort, and failure of the project artifact. Deciding which risk mitigating actions to pursue has largely been an intuitive endeavor, relying on expert opinions which are typically opaque. A more quantitative approach, based on results from actual past projects, is needed. This paper presents empirical findings relating past risk mitigating actions and project outcomes such as project cost, project schedule, and project risk. The findings are based on analysis of a legacy archive of project risk and risk mitigating actions from a large design organization, as well as from categorizing the different types of actions found in the archive based on a taxonomy developed using the archive itself, and analyzing the outcomes of those different types of actions. This study presents a more quantitative understanding of the relationship between a project state, the risks involved, and risk-mitigating actions taken during the project. This will enable improved decision making with better knowledge of the possible consequences of different types of risk mitigating actions and their effects in decreasing project risk.

Selection and/or peer-review under responsibility of Georgia Institute of Technology

Keywords: Risk mitigation; data mining; taxonomy; design informatics

1. Introduction

Understanding and managing project risk is an important aspect of any large and complex design endeavor. In this context, risk is defined as a state of uncertainty where a possible outcome can have an undesirable effect [1]. Thus, risk consists of two components: 1) uncertainty, where limited knowledge results in the inability to accurately or precisely understand the current state of the project or predict its eventual outcome or future state, and 2) undesirable effects, where an outcome can negatively affect the project. Inadequate consideration of risks can lead to

* Corresponding author.
E-mail address: rmalak@tamu.edu

Selection and/or peer-review under responsibility of Georgia Institute of Technology
doi:10.1016/j.procs.2013.01.088

wasted money, effort, and time, if the undesirable effects of risks come to fruition. They can also lead to other secondary effects, such as having to divert resources from other projects, decreasing an organization's reputation, hindering the organization's ability to pursue other opportunities such as additional contracts, or being able to take full advantage of market opportunities in a timely fashion.

Due to the potential negative effects of risk, there is strong motivation for project managers to obtain better models and information regarding the different risks that exist in a project, and to better understand how risk interacts with the different actions that stakeholders perform within a project. However, much of the existing literature on risk focuses on technical risk, such as the likelihood of individual components of a system failing and the effects of their failure on the system. Examples include Failure Modes and Effects Analysis (FMEA), Failure Modes, Effects, and Criticality Analysis (FMECA) [2], and probabilistic risk assessment techniques such as Fault Tree Analysis (FTA) and Event Tree Analysis (ETA) [3-6]. On the other hand, project risk includes additional factors such as the monetary cost of developing the technical artifact, manpower, schedule, and the opportunity cost of not pursuing other projects, in addition to the technical performance of the artifact. Although the two are related, they are not synonymous; for example, an organization could choose to use parallel development teams on a subsystem objective to reduce the project risk, even though the technical risk is not reduced.

Although technical risk may be a strong indicator of project risk, methods to treat technical risk may not apply equally well to project risk. For example, many methods for technical risk involve bottom-up approaches, such as determining the likelihood of component failures, and determining how the effect of their failure propagates throughout the rest of the system. With the complexity of many large-scale design projects, it may be impractical to directly apply such an approach. Furthermore, it is not clear that project risk metrics are directly analogous to technical risk metrics. While technical risks can be characterized to a certain extent by whether or not the artifact is able to still fulfill its objective despite the negative consequences of a risk (such as the ability of an airplane to remain flyable given the loss of an engine), a project does not necessarily fail per se (unless it is cancelled), but project risks instead lead to increased costs and delayed schedules.

To treat risk once it has been identified, there are four main categories of actions: risk avoidance, risk sharing, risk mitigation, and risk acceptance [7]. *Risk avoidance* is to circumvent events that carry the identified risk, such as by changing a production process such that the process step carrying the identified risk does not occur. *Risk sharing* is to transfer the risk to other parties, such as by outsourcing the production of a subsystem component, or to transfer the consequences of the risk, such as by purchasing insurance. *Risk mitigation* is to decrease the probability of the risk, and/or to decrease the consequences of the risk should it occur. *Risk acceptance* is to adapt to the risk should it occur, such as by creating contingency plans.

In a design project where the design organization has direct control over the risks, risk mitigation is often the most appropriate strategy for treating an identified risk [8]. Thus, risk mitigating actions is the primary focus of this study. Identifying which types of risk mitigating actions to use, and what sequence of them has the most impact on decreasing project risk, would help decisions makers in planning for a project, and in adapting to different project conditions as they occur.

To further this goal, we analyzed the contents of a legacy archive from a large engineering design organization. The contents of the archive are largely textual and were written by members of the organization about identified project risk issues while they worked to solve those issues. It contains reports describing risk issues that could substantially impact the project progress of developing a subsystem of a particular product model, and the actions of engineers who mitigated that particular risk.

We created a taxonomy discovery technique that directly used the archival information to populate its categories and did not require external sources, such as domain experts, other than an initial taxonomy with which to seed and start the discovery process [9]. The taxonomy discovery technique was used to refine a taxonomy that could adequately categorize the different types of risk mitigating actions observed in the archive. This paper presents results and insights gained from analyzing the archive using the developed taxonomy, and suggests improvements to any archive on project risk so that future archives can be more descriptive of ongoing projects, helping engineers to clarify the identified project risk and the effects of their risk mitigating actions on the risk. The improvements will also help in understanding the relationship between project risk and risk mitigating actions, to be able to better predict the effects of future risk mitigating actions.

2. Description of Legacy Archive

The legacy archive used for this study came from a large engineering design organization, which manufactures highly complex systems and has over 50,000 employees. It is termed *legacy* because the archive describes past risk issues and engineers' actions regarding them that have already occurred, and the engineers who generated the information are not available to clarify the text. The archive was based on a product development project which cost billions of dollars involving multiple factories in different countries and spanned over a decade, although the archive contents themselves spanned a period of 3 years. The archive contains reports on issues that posed a significant risk to subsystems of this product, as well as the actions of the engineers in working to decrease that risk. There were a total of 185 reports in the archive. Of those reports, 68 merely detailed an identified risk without listing any risk mitigating actions and so were excluded from the study. The remaining 117 reports contained a total of 822 entries.

Each report entry contained a textual description of the risk, an evaluation of the current risk likelihood and risk consequence levels, and the rationale for their assignment. It also contains a list of planned actions to treat the risk, with details such as their planned completion dates, the criteria for evaluating their success, new risk levels if they're successful, and each action's success or failure after it has been executed and evaluated. There is also other identifying information such as the department or team responsible for the particular issue. Figure 1 shows the layout of a typical report entry in the archive.

Different engineers in different development teams contributed to the archive throughout its history. Although they may have been instructed to record specific information about a project, the thoroughness of the information recorded can vary among different personnel, and they may not necessarily adhere to well-defined semantics. This increases the difficulty of extracting useful content from this archive [10-12]. In this archive, the recorded information largely describes the actions that engineers performed, but not their rationale, alternatives considered, evaluation criteria for which of the possible alternative actions to pursue, or other information that would be relevant for understanding their thought process in deciding what they expected may be the most effective actions. The archive is thus a design history archive as identified by Rockwell et al. [13], rather than a design rationale archive. This distinction is important in that a design rationale archive captures the thought process behind the decisions and actions in an project, allowing for greater understanding of the context of each action, while a design history archive simply captures the outputs of that thought process, the actions themselves. This context can be highly beneficial for retrospective analysis.

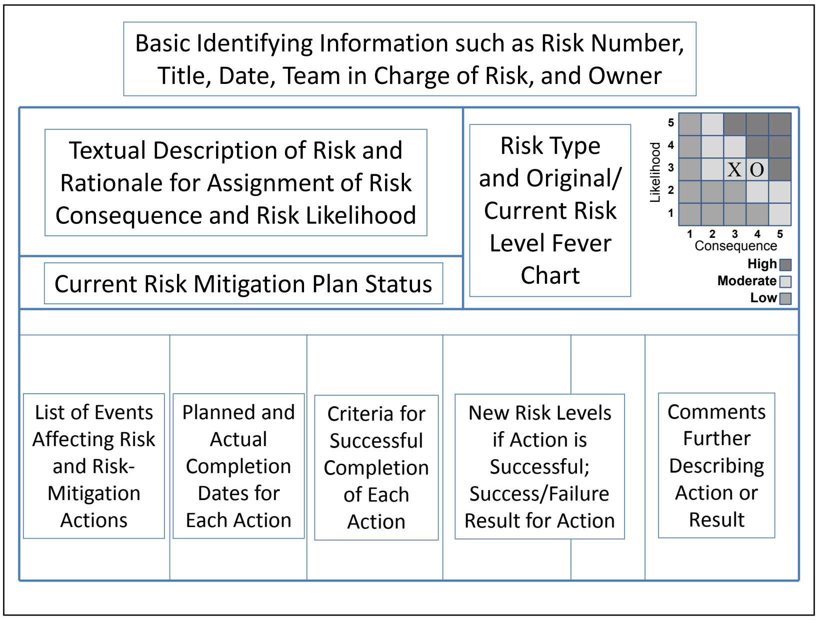

Fig. 1. Example layout of a risk report entry.

3. Taxonomy of Risk Mitigating Actions

A taxonomy is a hierarchical arrangement of concepts [14]. Each concept has a description to clarify its definition. A taxonomy of risk mitigating actions for describing entries in the legacy archive in this study was developed using a taxonomy discovery technique that used the archive itself as an input as well as an initial taxonomy as a seed, but otherwise did not require any external sources [9]. The necessity of this technique on this archive was due to its legacy nature, which meant that the original engineers who authored the entries in the archive were inaccessible for clarification of the text or understanding their thought process behind the actions they executed. An advantage of this technique is that the taxonomy reflects the content of the archive more directly, as opposed to taxonomies that are based on expert opinion, which may differ from conventions used by practicing engineers, or taxonomies based on archive guidelines, which engineers may have adhered to with varying quality depending on training and expediency.

The initial seed taxonomy used for this research was presented by Coughlan and Coghlan [15] in their work on action research. After a survey of existing risk mitigating action literature, their taxonomy of risk mitigating actions was judged the most applicable for this study. However, it was heavily modified to better fit this particular archive.

Once the taxonomy was refined, it was used to categorize all 822 entries in the archive.

3.1. Summary of taxonomy discovery technique

The taxonomy discovery technique involves two or more (human) coders, though two were used as primary coders in this study, with a third as a “naïve coder” to ensure the taxonomy was properly defined. In the context of this study, *coding* refers to the qualitative research process of adding descriptive markers or codes to segments of text [16]. Coding can be applied to interviews, reflexive journals, design notebooks, and a variety of other media where information is primarily in textual form, to categorize and externalize the meaning within the text so that it can be computer-interpreted and statistically analyzed.

The two coders used a taxonomy to independently code a set of entries. On the first iteration, the taxonomy that they used was the initial taxonomy to seed this process, but for each iteration thereafter they used the most recent version of the taxonomy. They then compared the codes that they had assigned to each segment of text. If the codes did not match then they discussed the reasons behind how they assigned the codes and the reasons for the mismatch.

One of the possible reasons for a mismatch was if the taxonomy was inadequate. For example, several codes may have been too broadly defined, leading the coders to use two different codes to describe the same action. In these situations, the two coders discussed how to redefine the codes to avoid mismatches in the future, and updated the taxonomy accordingly. Other reasons for a mismatch were if the archive lacked sufficient contextual detail for an accurate coding attempt, or if one of the coders did not properly understand some of the information presented in the archive. In the latter case, discussion focused on coder instruction.

The coders then coded a new section of text using the updated taxonomy, and repeated this process until very few mismatches due to the taxonomy were found. At that point the taxonomy refinement was considered complete and they used the refined taxonomy to code the rest of the archive.

3.2. Final version of taxonomy of risk mitigating actions

The top level of the taxonomy is whether an entry was an *Action*, carried out by the design organization to mitigate the risk, or an *Event*, which affected the project and its risk levels but was an external influence and not under the direct control of the design organization. An organization can choose among different actions when deciding on how to mitigate a risk, but events are an outside force affecting the risk around which the organization must prepare. The organization may have some influence over events, but it does not exert direct control on them. An example of an event is regulatory safety approval of the seat of a vehicle. Although the organization can influence the outcome of this event, by investing in better design or better materials, it does not directly decide on whether or not a particular design is approved by the regulatory agency. In this study, the focus is on risk mitigating actions, so events, other than being categorized as such, were not decomposed further.

Each entry in the archive, if categorized as an action, had two further codes assigned to it: an embodiment code, describing how the action was carried out, and a purpose code, describing the reason for the action and how it was intended to mitigate the risk. Thus, the code for each action entry consisted of an embodiment-purpose tuple, such as *Coordinate-Gather_Data* to describe multiple departments working together to gain insight into how to tackle the risk, or *Request-Approval* to describe sending information to another entity for approval with an expectation of a reply. Table 1 gives a summary and an example of the different categories under each action attribute. Because there are 4 different embodiment codes and 7 different purpose codes, there are a total of 28 possible code combinations that can be assigned to an action. In addition, an *Event* code could be assigned, for a total of 29 different codes under this taxonomy. During the refinement process, an additional *Other* code was occasionally assigned to an action purpose, to indicate actions whose purposes were not contained by the taxonomy, but by the end of the process the taxonomy purpose definitions had been refined to encompass all observed actions, so it was excluded from the table.

3.3. Validation of taxonomy discovery technique

Validation of the taxonomy was carried out using inter-rater reliability as a metric, or how often the two coders assigned the same codes to segments of text. Although consistency does not necessarily entail accuracy, it gave a level of confidence in the coding results and the taxonomy. In this study, the inter-rater reliability for the final taxonomy was 62.2%, and a Cohen's kappa [17, 18] of 0.556, which is considered fair to good for qualitative research coding [19, 20]. Validation was also carried out by analyzing how often mismatches were due to the taxonomy, as opposed to being due to the archive or the coders. Near the end of the taxonomy refinement process, very few mismatches were due to the taxonomy; 67% of the mismatches were due to ambiguities in the archive entries themselves, while the remaining mismatches were due to a coder misinterpreting the archive information.

A further validation step was to use a naïve coder, so-called because he was not a part of the taxonomy refinement process and thus did not know the rationale behind the definitions used in the taxonomy [21]. During the taxonomy refinement process, it was possible that the two primary coders refining the taxonomy had high match rates because they came to intuitively understand the codes that each other were likely to assign to a segment of text. In other words, their inter-rater reliability may have been due to their tacit understanding, rather than what was explicitly defined by the taxonomy. To check for this, once the taxonomy was refined and considered ready for use, the naïve coder was given the taxonomy definitions and a few examples to familiarize him with the coding process, and was then given a section of the text to code. If the taxonomy were properly defined, then his inter-rater reliability scores with the primary coders would be similar to their scores with each other. This was found to be the case in the study, where the naïve coder had an inter-rater reliability of 68.3% and a Cohen's kappa of 0.628, indicating that the taxonomy captured the explicit knowledge of the coders.

Table 1. Taxonomy of risk mitigating actions

Attribute	Category	Description	Example
Embodiment	Inform	Primarily one-way transfer of information	"Hold a risk understanding meeting"
	Coordinate	Multiple departments working together on action	"Develop plan with X Department"
	Request	Transfer of data with expectation of reply	"Submit plan for approval"
	Typical	No special embodiment of action	"Determine temperature at point X"
Purpose	Gather_Data	Gathering prior knowledge or observations	"Measure current noise levels"
	Resource_Planning	Allocation of manpower and scheduling	"Form Weight Focus Team"
	Technical_Evaluation	Technical analysis and decision making	"Perform trade off study for method to reduce load"
	Technical_Planning	Planning requiring technical analysis	"Set weight reduction goal based on materials/structures analysis"
	Approval	Obtaining consent for an action from another entity	"Program approval of load reduction method"
	Implementation	Executing a previously decided plan or process	"Make Build/Revise kits"
	Validation_and_Testing	Verifying effect of action or implementation	"Review material results"

Table 2. Archive action totals

Purpose	Typical	Inform	Request	Coordinate	% of Actions
Gather_Data	44	20	10	6	10.8%
Resource_Planning	159	13	2	47	29.7%
Technical_Evaluation	158	2	2	29	25.6%
Technical_Planning	74	1	1	33	14.6%
Approval	1	1	31	31	8.6%
Implementation	47	0	1	3	6.8%
Validation_and_Testing	27	0	0	2	3.9%

4. Results and Discussion

Out of the 822 entries that were in the archive, 77 were events and were not categorized further. Table 2 gives a breakdown of the embodiment-purpose totals for the remaining 745 actions. The purpose codes are listed in the rough order that they would be expected to occur while solving a risk issue, while the embodiment codes are listed in order of the amount of interaction with other departments or entities involved.

A majority of actions (55.3%) were in the *Resource_Planning* and *Technical_Evaluation* categories alone. By contrast, only 10.8% of actions involved making changes that will directly affect project risk, namely *Implementation* of changes and *Validation_and_Testing*. This indicates that engineers spend a great deal of time analyzing and discussing a risk issue when it is identified.

An empirical result from this study is that engineers tended to coordinate with other departments more often during the initial data-gathering and planning phases, with much less coordination among departments needed as the planned actions are executed toward the end of risk mitigation. It was somewhat surprising that in a large engineering design organization, implementing changes to a design and testing the change after implementation did not require much coordination among departments despite the complexity of the project.

Each entry in the archive contained a success criterion to gauge whether or not the action (or event) was successful, and also the result of that measurement. The result was blank if the action had not been completed. Out of the 745 actions, a total of 548 actions were completed and had a success or failure conclusion. Table 3 gives the breakdown of those actions relative to the action's embodiment. In general, actions were about 88% successful. The one exception was *Inform* actions, of which only one failure was recorded out of 28. This however is not surprising; the *Inform* embodiment code is defined as a one-way transfer of information, such as holding a training workshop, and those will typically be considered a success as long as they are held.

Table 4 gives the breakdown of an action's success relative to the action's purpose. Although an action on average succeeded 88% of the time, *Technical_Evaluation* failed about 20% of the time, meaning that the engineers found problems with the proposed risk mitigation solution only once they started conducting detailed computer simulation studies. Also, 26% of *Validation_and_Testing* failed, which again indicates that problems with the proposed solution were found only at the latter stages of the risk mitigation process. In this case, failure of a validation action does not indicate that the action itself failed but that the solution was not validated. A substantial amount of solution failures were not discovered until final testing after implementation, although it should be noted that the sample size was low. Since many reports did not contain a validation step, it is possible that validation was conducted only in the riskiest circumstances, leading to the relatively low success rate observed.

Table 3. Action success by embodiment

Embodiment	Success	Failure	% Success
Typical	318	45	87.6%
Inform	27	1	96.4%
Request	32	4	88.9%
Coordinate	106	15	87.6%

Table 4. Action success by purpose

Purpose	Success	Failure	% Success
Gather_Data	54	6	90.0%
Resource_Planning	157	14	91.8%
Technical_Evaluation	106	27	79.7%
Technical_Planning	75	8	90.4%
Approval	43	4	91.5%
Implementation	34	1	97.1%
Validation_and_Testing	14	5	73.7%

Table 5. Action success by report visibility

Visibility	Success	Failure	% Success
Executive	49	2	96.1%
Program	222	24	90.2%
Integration	208	34	86.0%
Local	50	16	75.8%

Each of the 118 risk reports analyzed contained a rating of the visibility or possible scope of effect or review of the risk. The visibility rating ranged from the highest, executive, to the lowest, local. The number of successful or failed actions within each report was tabulated according to the visibility rating of that report, with the results given in Table 5. Although not unexpected, the reports contained less unsuccessful actions if the level of review for the risk increases. This may reflect more resources devoted to mitigating the risk if it has a higher impact or greater engineer risk aversion toward trying potentially risky solutions if the level of scrutiny increases.

Of the 77 observed events, 57 had success or failure recorded. Out of those 57, 46 were successful, indicating a success rate of 80.7%. An example of a failed event would be if a regulatory agency rejected the proposed solution for mitigating the risk. That the success rate for events was lower than that for actions is not particularly surprising, since the organization does not have direct control over events, which by definition are controlled by outside entities. However, this does indicate that more resources could be spent on improving the success rate of events so that they do not adversely affect risk mitigation.

5. Recommendations for Improving the Archive

In working with a legacy archive, the limitations of the archive and the possibilities for improvement were very apparent. Although the specific taxonomy produced by the taxonomy discovery technique in this study will vary depending on the archive to which it is applied, these recommendations should be applicable to most project archives, especially ones that record details regarding project risk and risk mitigating actions.

5.1. Design history archive vs design rationale archive

The archive used for this study was a design history archive, focusing primarily on recording the actions that engineers took while mitigating project risk. A design rationale archive by contrast also records the engineer's reasoning behind the actions, the alternatives considered, and other aspects of the risk mitigation thought process. Such an archive would be a lot more useful for retrospective analysis in understanding how engineers went about solving problems, and also in diagnosing which approaches tended to work better than others. This would be invaluable for large scale statistical analysis of risk databases, to determine the most promising approaches for mitigating risk in a given project state or situation. By having engineers document their rationale, a design rationale database would also encourage engineers to think through the risk mitigating actions that they are proposing, improving the quality of their work.

5.2. Consistent terminology

Many different engineers contributed to the archive. However, many of them used the same word to mean different things, as well as using different words to mean the same thing. For example, the word "identify" was often encountered, but it could refer to gathering data, such as "identify all previous risk reports related to current risk", or to technical analysis, such as "identify an optimal solution", or to planning and scheduling, such as "identify an acceptable test schedule". In many cases it is difficult to determine the purpose of the action due to such words. Other similar words included "design", "develop", and "review".

Developing a set of terminology to be used across the organization would greatly simplify analysis of the database. In this study, the analysis was manual in nature, but a more large-scale study to extract risk and risk mitigating action relationships of a more statistical significance would likely need to be automated. Despite the development of ontologies to describe the project design process and project risk, the use of such words can make it difficult to extract accurate descriptions of the archival content.

5.3. Structured archive

Although the legacy archive had a variety of different fields to input different items relating to a project risk issue, the content of each field varied greatly from report to report. Thus, codifying the actions required searching in multiple fields to extract enough contextual information for an accurate classification. A more structured archive could capture the information in a more well-defined way, making it easier to ascertain and reconstruct the decisions and actions that occurred during risk mitigation.

For retrospective analysis, the ideal project risk archive would contain enough content to understand the project and various project factors such as its schedule, a listing of the decisions and actions during the project, their rationale, intended effect, and actual resultant effects on the project. The content should also be in an easily extracted form, so that automated data mining techniques can be used to determine the most beneficial actions to execute in a given situation. These recommendations will help improve archives toward that goal.

6. Conclusion

This paper presented results and insights on project risk and risk mitigating actions gained from analyzing a legacy risk archive from a large design organization. It also presented techniques that do not rely on external sources beyond an initial taxonomy that can be used for classifying information in an archive that is largely unstructured and textual in nature. Recommendations for improving future similar archives are also presented. Further study into such archives can help improve understanding of the interaction between risk and risk mitigating actions, allowing for better decision making of actions in future projects.

Acknowledgements

This material is based upon work supported by the National Science Foundation under Grant No. CMMI-1029964. Opinions expressed in this paper are of the authors and do not necessarily reflect the views of the National Science Foundation.

References

1. D. P. Thunnissen, Uncertainty Classification for the Design and Development of Complex Systems, presented at the 3rd Annual Predictive Methods Conference, Newport Beach, CA, 2003.
2. D. H. Stamatis, Failure Mode and Effect Analysis: FMEA from Theory to Execution. Milwaukee: ASQ Quality Press, 2003.
3. W. E. Vesely, F. F. Goldberg, N. H. Roberts and D. F. Haasl, The Fault Tree Handbook, US Nuclear Regulatory Commission, Washington, DC, 1981.
4. M. A. Greenfield, NASA's Use of Quantitative Risk Assessment for Safety Upgrades, presented at the IAAA Symposium, Rio de Janeiro, Brazil, 2000.
5. T. Bedford and R. M. Cooke, Probabilistic Risk Analysis: Foundations and Methods. Cambridge: Cambridge University Press, 2001.
6. M. Stamatelatos and G. Apostolakis, Probabilistic Risk Assessment Procedures Guide for NASA Managers and Practitioners v 1.1, NASA, Safety and Mission Assurance, Washington, D.C., 2002.
7. M. Muehlen and D. Ho, Risk Management in the BPM Lifecycle, in Business Process Management Workshops. vol. 3812, C. Bussler and A. Haller, Eds., ed Berlin / Heidelberg: Springer, 2006, pp. 454-466.
8. R. Miller and D. Lessard, International Journal of Project Management 19 (2001) 437-443.
9. C. Hsiao, M. Ruffino, R. Malak, I. Y. Tumer and T. Doolen, Developing a Taxonomy of Risk-Mitigating Actions from a Legacy Database of a Large Design Organization, presented at the ASME International Design Engineering Technical Conference & Computers and Information in Engineering Conference, Chicago, IL, 2012.
10. S. Salzberg and M. Watkins, Research in Engineering Design 2 (1990) 35-52.
11. M. Hertzum and A. M. Pejtersen, Information Processing and Management 36 (2000) 761-778.
12. C. McMahon, A. Lowe, S. J. Culley, M. Corderoy, R. Crossland, T. Shah and D. Stewart, ASME Journal of Computing and Information Science in Engineering 4 (2004) 329-338.
13. J. A. Rockwell, I. R. Grosse, S. Krishnamurty and J. C. Wileden, ASME Journal of Computing and Information Science in Engineering 10 (2010) 031008.
14. A. Gilchrist, Journal of Documentation 59 (2003) 7-18.
15. P. Coughlan and D. Coghlan, International Journal of Operations & Production Management 22 (2002) 220-240.
16. C. F. Auerbach and L. B. Silverstein, Qualitative Data: An Introduction to Coding and Analysis. New York: New York University Press, 2003.
17. J. Cohen, Educational and Psychological Measurement 20 (1960) 37-46.
18. P. F. Brennan and B. J. Hays, Research in Nursing & Health 15 (1992) 153-158.
19. J. R. Landis and G. G. Koch, Biometrics 33 (1977) 159-174.
20. C. Robson, Real World Research: A Resource for Social Scientists and Practitioner-Researchers. Cambridge: Blackwell, 1993.
21. S. Ahmed, S. Kim and K. M. Wallace, ASME Journal of Computing Information Science and Engineering 7 (2007) 132-140.